



Derült égből antivírus,
avagy a felhőalapú védelem
árnyas oldalai



Bemutakozás

Buherátor

Silent Signal

IT biztonsági szakértő

OSCP, GWAPT

buherator@silentsignal.hu



Bevezető

- Tartalom
 - Mi az a Cloud AV?
 - Támadói modell
 - Támadások
 - Mérlegelés
- Célok
 - Főbb kockázatok bemutatása
 - Segítség termékválasztáshoz
 - Kutatás ösztönzése

Korábbi munkák

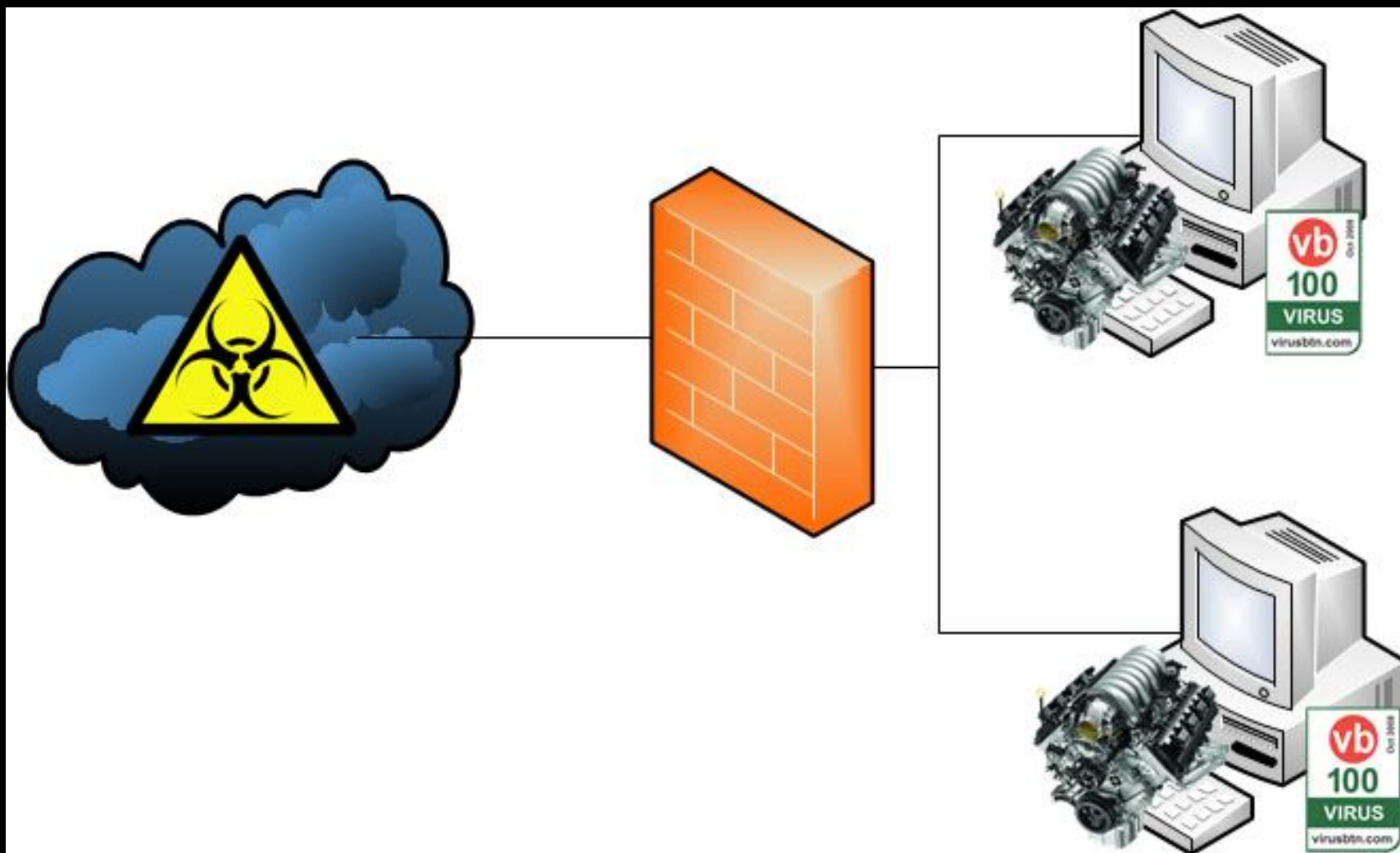
Oberheide-Cooke-Jahanian:

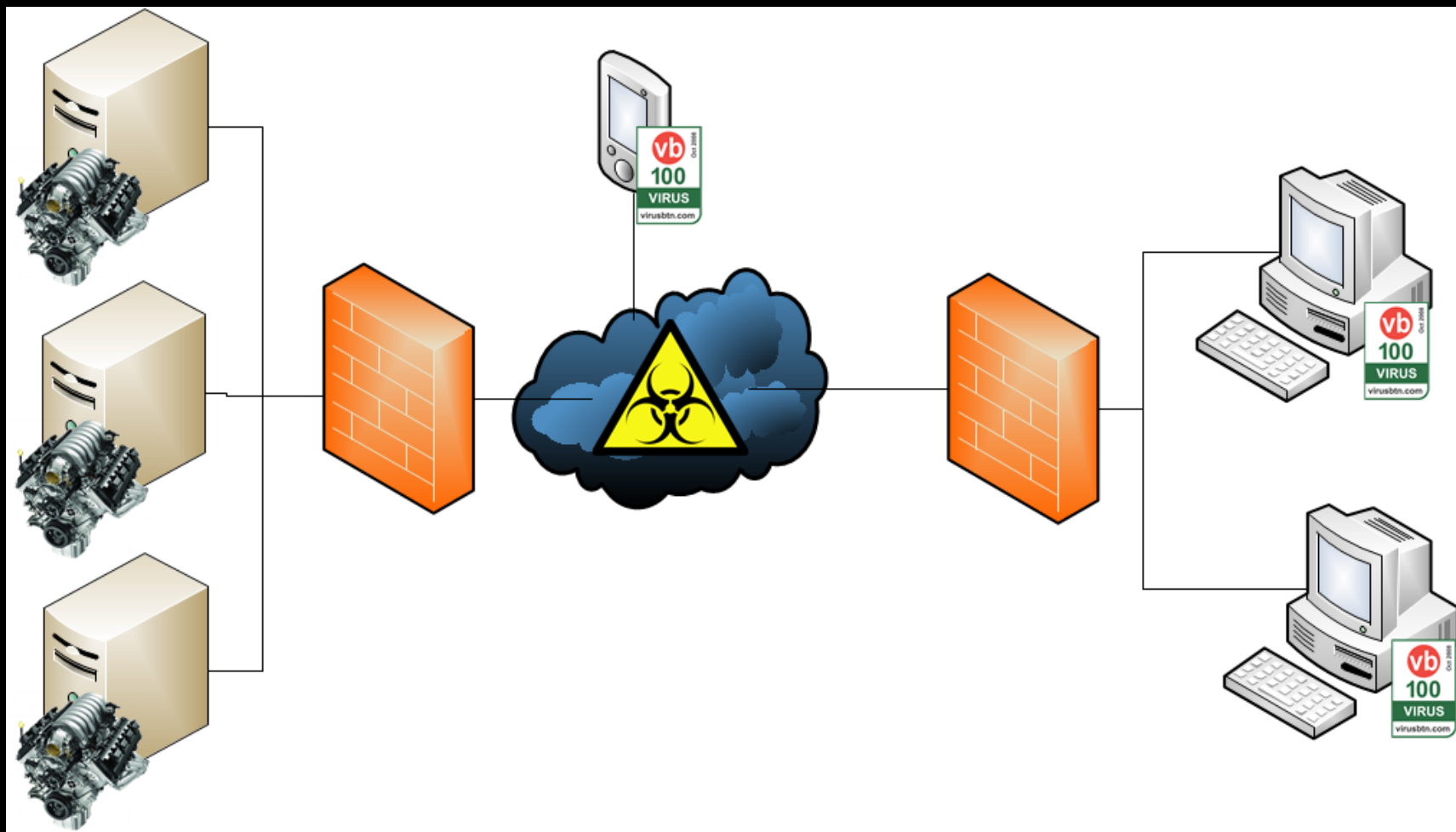
CloudAV: N-Version Antivirus in the Network Cloud

Krasznay Csaba:

Ipari felhő infrastruktúrák a gyakorlatban

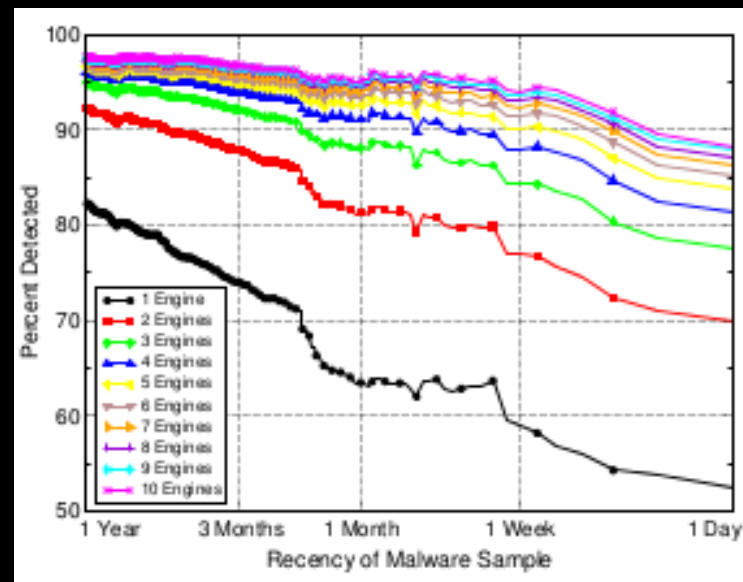




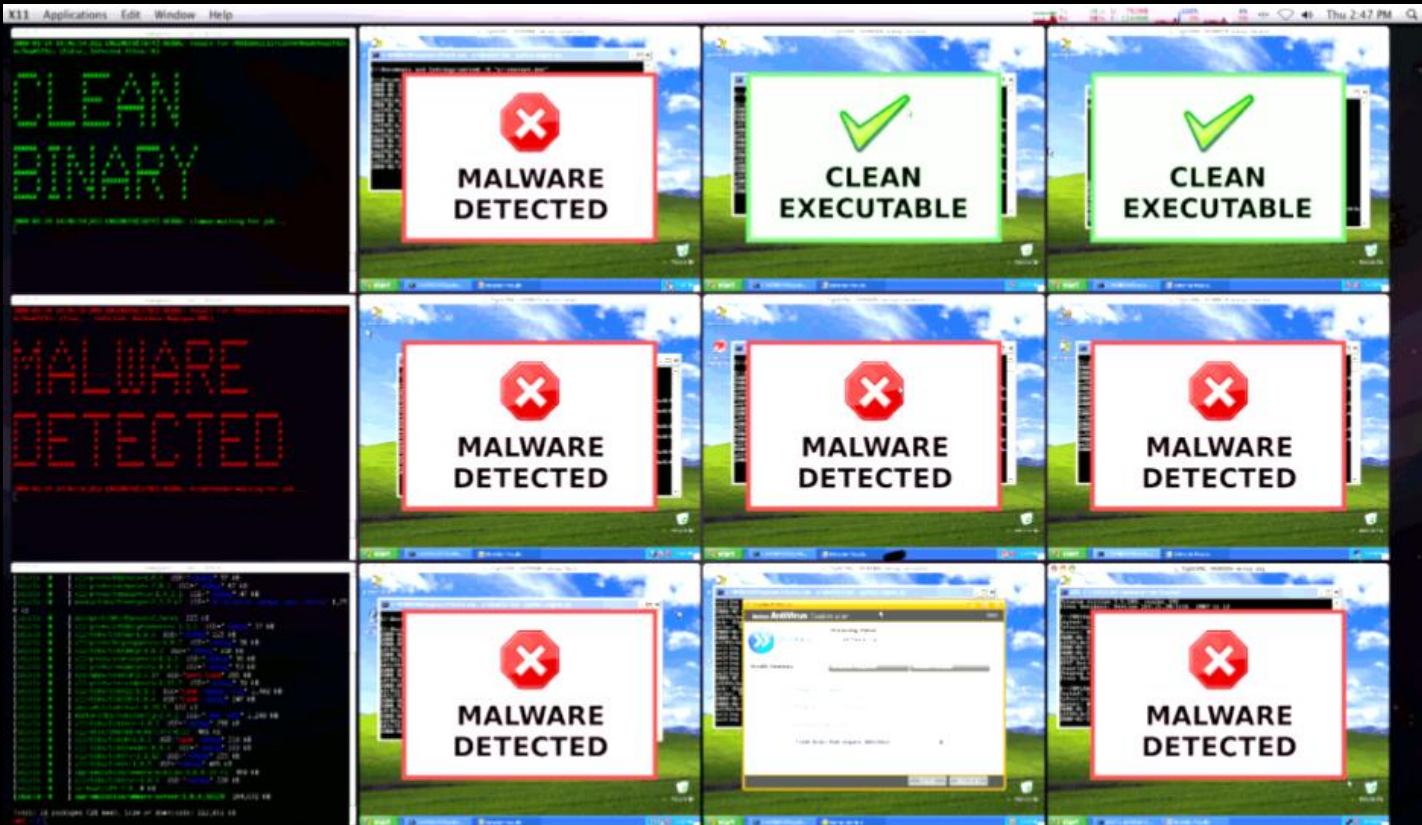


CloudAV

- Teljesítmény
- Reputációalapú heurisztika
- "N-verziós védelem"
 - Jobb találatarány
- Központosított menedzsment
- Kisebb támadási felület (AV sérülékenységek)
- Mobilitás
- Nyomrögztítés
 - "Retrospektív detekció"



Proof-of-Concept



© Jon Oberheide

Gyakorlat :)

```
b@buttercup:~/projects/cloudAV$ head -n 34 gdata/cloudsecurity@gdata.de/modules/requesturl.js |  
tail -n 13  
function RequestUrl_Builtin(aUrl)  
{  
    // CSDebug.logInfo("WorkUrl.SampleRequest url:"+aUrl);  
  
    let Milliseconds=50;    // simulate work in ms  
    // SleepEx  
    let date=new Date();  
    let curDate=null;  
    do  
        curDate=new Date();  
    while(curDate-date<Milliseconds);  
    //
```



Támadói modell

- Elsődleges cél: AV -> Belépési pont
- Aktív hálózati támadó
 - Az Internet veszélyes hely
 - A célpont vállalati hálózata megbízható
 - Az AV cloud megbízható
 - A mobil kliensek megbízhatatlan hálózatokat használhatnak
- Public AV cloud
- A végponti védelem már települt

Az Internet veszélyes hely

- Mobil kliensek WLAN HotSpot-on
 - Rogue AP
 - WPAD
- DNS
- Köztes hopok
 - ISP-k
- BGP?



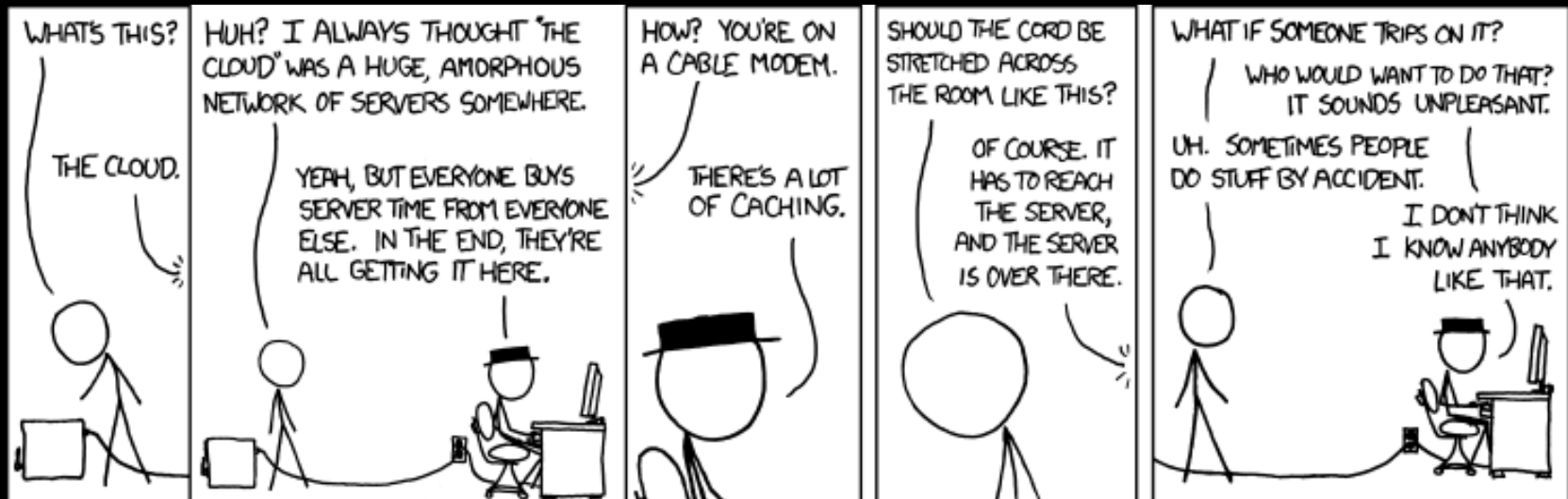
Rendelkezésreállítás

Szolgáltatói SLA-k...

- Lásd még: Azure

(D)DoS

- Ügyfélproxy
- DNS
- ~~OCSP~~
- AV szolgáltató



DEMO



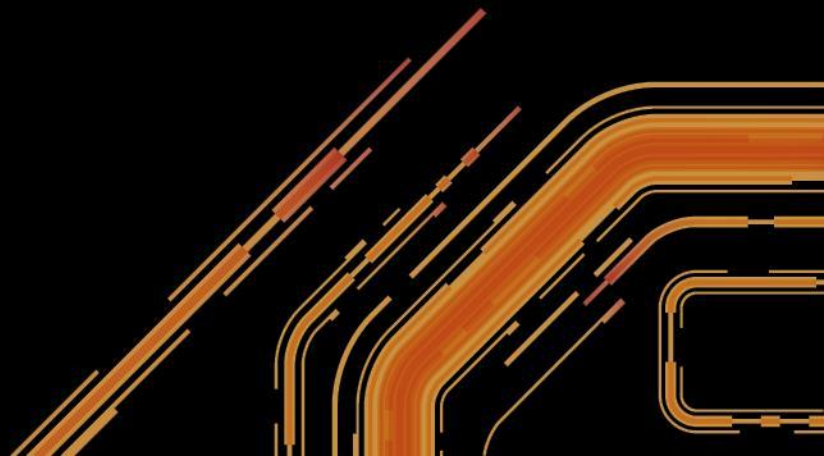
Rendelkezésreállítás

- Policy kérdés
 - a) Nincs válasz a felhőből => Tiszta
 - b) Új alkalmazás/dokumentum/... csak működő kapcsolat esetén nyitható
 - c) ...
- Caching
- Cloud -> kiegészítő funkció
 - Offline szignatúrák
 - Teljesítmény?



Integritásvédelem

- Szignatúrafrissítések
- Szoftverfrissítések
 - Akár néhány naponta
- *Kezdeti terítés*
- Biztonsági szoftver => magas jogosultság
- Kommunikáció HTTP alapon
 - Jól proxyzható
- Integritásvédelem
 - TLS
 - Code signing



DEMO



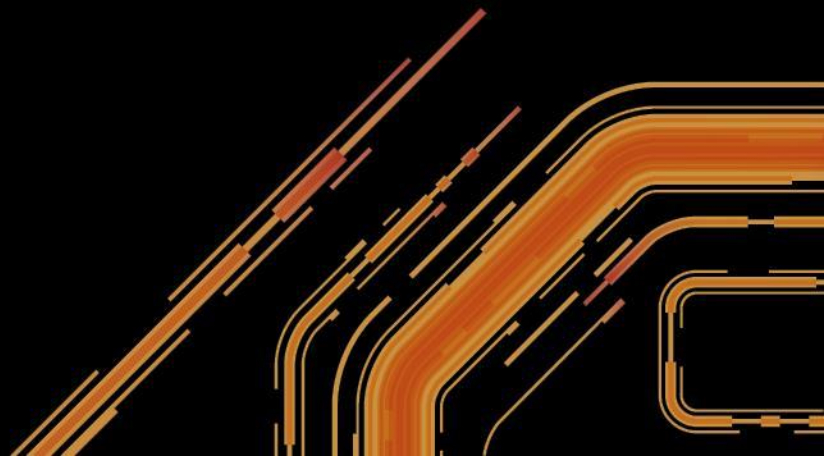
Integritásvédelem

- Nem csak CloudAV-probléma
 - Alapvetően implementációs kérdés
- TLS nem mindig használható
- Code signing nem az igazi erre az alkalmazásra
- Private Cloud?



CloudAV==SPoF ?

- A támadók racionális gazdasági döntéseket hoznak
- CloudAV => Sok ügyfél => Nagy haszon
- Mennyire bízhatunk a gyártókban?



Performance Against Enterprise Policy by Application Purpose

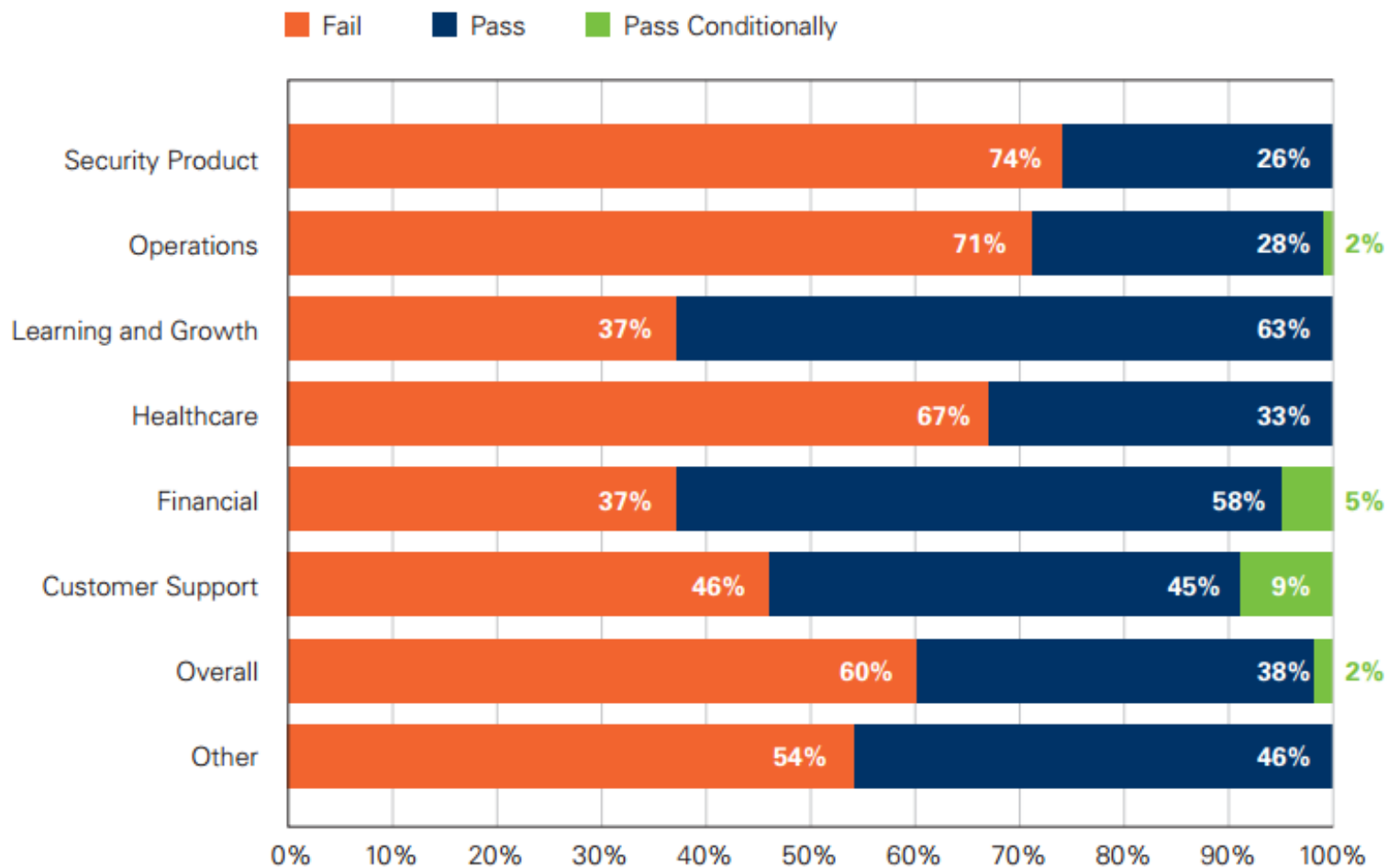


Figure 15: Performance Against Enterprise Policy by Application Purpose

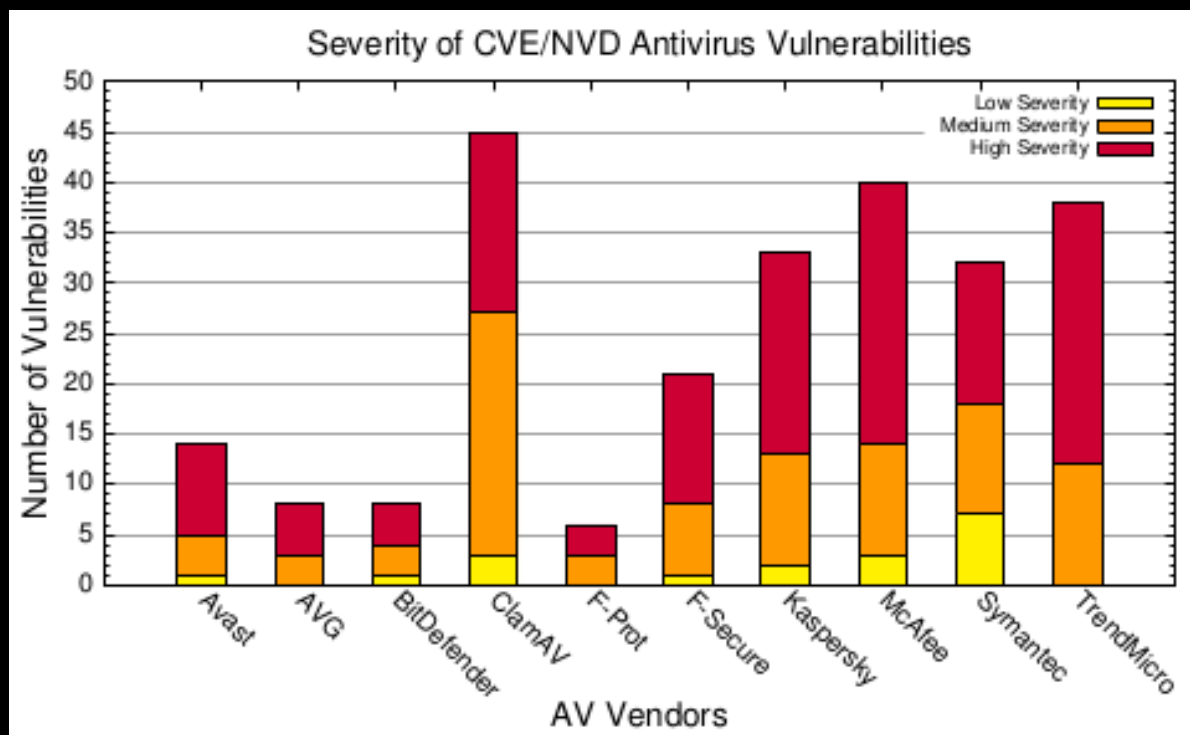
DEMO





CloudAV==SPoF ?

- Bizalmi kérdés
- A security vendorok is hibáznak



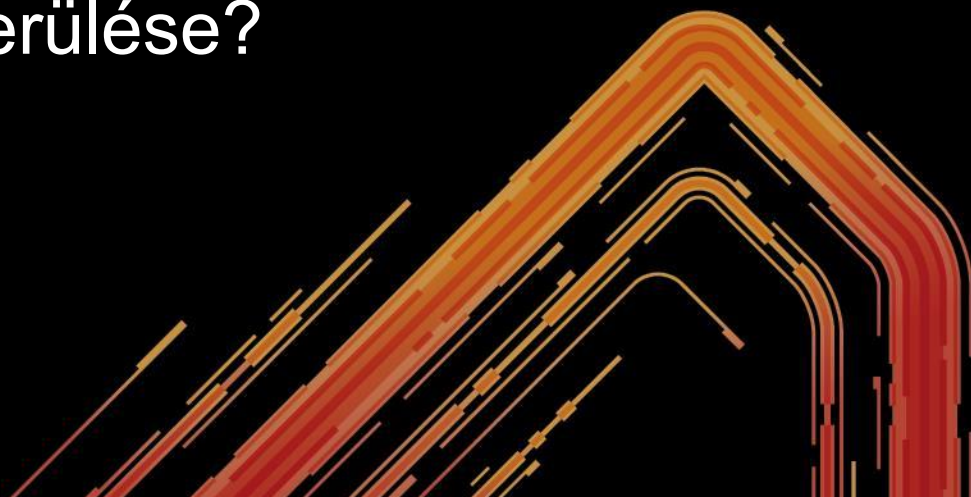
CloudAV==SPoF ?

- Bizalmi kérdés
- A security vendorok is hibáznak
 - De nem reklámozzák...



Bizalmasság

- Üzleti titkok a felhőben?
- A CloudAV-k általában csak lenyomatokat/mintákat küldenek haza
 - Bizalmasság megmarad
 - Megmarad?
 - Detekció megkerülése?

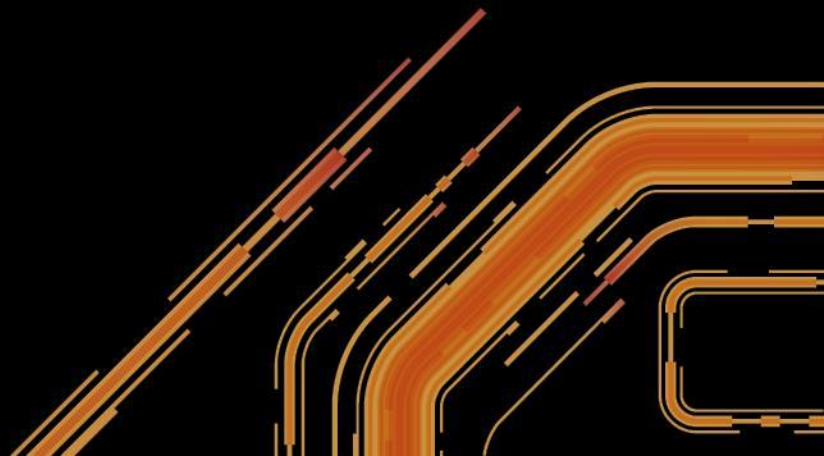


CloudAV

- ~~Teljesítmény~~
- Reputációalapú heurisztika
- ~~"N-verziós védelem"~~
- Központosított menedzsment
- ~~Kisebb támadási felület
(AV sérülékenységek)~~
- Mobilitás
- Nyomrögztítés
- Függés a felhőtől
- Privacy vs. Pontosság

Konklúzió

- CloudAV => kiegészítő szolgáltatás
- Security-as-a-Service: elsősorban üzleti, nem technológiai modell
- A gyártók sem tévedhetetlenek
- Gazdag kutatási terület



The background features a complex pattern of glowing, multi-layered lines in shades of red and orange. These lines form a network of paths, some straight and others curved, creating a sense of movement and connectivity. The lines are set against a solid black background, which makes the vibrant colors stand out. The overall effect is reminiscent of a stylized circuit board or a data network map.

Köszönöm a figyelmet!

Külön köszönet: Dr. Csigusz, Infosec Reactions, Z

Linkek

<http://securityreactions.tumblr.com/>

<http://www.eecs.umich.edu/fjgroup/cloudav/>

http://krasznay.hu/presentation/openacademy_krasznay.ppt

<http://info.veracode.com/rs/veracode/images/VERACODE-SOSS-V4.PDF>

Marosi Attila @ Ethical Hacking 2013 ? :)



17:30-tól Buhera sörözés!

No Name Pub

1084, Tompa u. 8.

(a Mester utcai villamosmegállónál)